Colin R. Kass (*pro hac vice*)
PROSKAUER ROSE LLP
1001 Pennsylvania Ave., N.W.
Washington, D.C. 20004
(202) 416-6890
ckass@proskauer.com

David A. Munkittrick (*pro hac vice*)
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
(212) 969-3000
dmunkittrick@proskauer.com

Attorneys for Defendant Bright Data Ltd.
Additional counsel listed on signature page.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

X CORP., Plaintiff, v. BRIGHT DATA LTD., Defendant.	**PUBLIC VERSION** Case No. 23-cv-03698-WHA Hon. William A. Alsup Courtroom 12 – 19th Floor September 26, 2024, 8:00 a.m.

BRIGHT DATA'S OPPOSITION TO X'S MOTION FOR LEAVE TO AMEND THE COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES[1]

[1] Unless otherwise specified, all emphasis added, initial capitalizations conformed without brackets, and internal citations and quotation marks omitted.

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION.

In its Dismissal Order, this Court established a two-part framework for analyzing X's claims: Access and Scraping. X now returns to Court pleading to revive its claims. But it adds no new factual heft to its deficient allegations.

For its Access Claims, X still does not cite a single injury caused by Bright Data. It says that doesn't matter because Bright Data is a big scraper in a sea of scrapers, so any scraping-related harm should be attributed to Bright Data. We need not address that syllogism here, because even so, X's claims fail, since it has not alleged ***any*** injury from the whole lot of scrapers that have ever accessed X's platform.

As this Court explained, there is a fundamental difference between access designed to cause a denial-of-service or other server failure, and access that may be undesired but nonetheless depends on X's platform functioning as intended. The former may state a claim, but the latter does not. Here, X alleges no server failures. It claims it spent money on server farms to operate its social media platform, which has successfully handled all requests – wanted or unwanted – with aplomb. Its allegation that it would buy fewer servers if it could eradicate unwanted server requests is not an interference with *property*. It is the opposite: an allegation that its servers worked exactly as intended. That dooms X's Access Claims.

X's attempt to revive its preempted Scraping Claims fare even worse. It does not pretend to present new facts. Instead, it just "disagree[s]" with this Court's ruling, and asks the Court to re-consider. In its view, X's use of state law to create a rival, dueling regime to block the unwanted reproduction and sale of social media content does not interfere with the Copyright Act's *exclusive* allocation of those rights, and furthers some amorphous privacy, security, or consumer protection state interest. But the Court already found otherwise.

That X "now disclaims any attempt to enforce X's users' copyrights" is irrelevant. It never sought to do that. What it tried to do was to use state law to exercise control over the reproduction and sale of information *it does not own*. That conflicts with the Copyright Act. Nor can X salvage claims dealing with non-user generated data, such as the *number* of likes or posts. The States, X says, are the *sole* sovereign regulator of this content because the Constitution renders Congress impotent to act with respect to facts and figures. That too is untrue, and contrary to this Court's Dismissal Order and the legions of cases that hold otherwise.

With conflicts rife and readily apparent, the preemption analysis should end there. But in a strange form of reverse preemption, X argues that these conflicts do not matter because the State has an overriding interest in preventing scraping. It launches into a one-sided diatribe against the practice. But it did this before, and it did not convince the Court. Nor has it convinced the California legislature. California has not made scraping illegal, and none of the state laws sued upon were designed to give X an information monopoly over public content on its site under the guise of protecting consumers, privacy, or data systems.

Leave to amend X's state law claims should be denied.[2]

II. X'S AMENDMENTS TO ITS PRIOR ACCESS CLAIMS ARE FUTILE.

A. X's Amendment to its Trespass to Chattels Claim is Futile.

1. *X Does Not Cure Its Deficient Allegations of Injury.*

This Court previously rejected X's "threadbare" allegation that Bright Data "impaired [the] condition, quality, and value of its servers" or "diminished the server capacity that X Corp. can devote to its legitimate users." Order 8-9 (ECF 83). Yet in response, X begins its motion by repeating identical statements – that automated access "diminishes X's server capacity," "degrades its user experience," and "strain[s] … its infrastructure." X Br. 4-6. After several iterations of this, it proclaims its "new allegations remedy the Court's concern." *Id.* But its pronouncement does not make it so. The "additional allegations merely reiterate and embroider the claims … already presented in [the] original complaint, adding little, if anything, of substance to [its] case." *Coleman v. Ramada Hotel Operating Co.*, 933 F.2d 470, 473 (7th Cir. 1991).

The Court's Dismissal Order sets the parameters for the types of injuries that establish a deprivation of personal property. "Denial-of-service attacks could prove remediable," the Court explained, but sending "requests to X Corp. servers in violation of the Terms … does not itself

[2] In addition to trying to resurrect its prior state law claims, X asserts three new claims. Because those have not been previously briefed, and do not have the benefit of a prior ruling, Bright Data believes that those claims are better addressed under Rule 12(b)(6). As such, we limit our opposition to the six state law claims X originally asserted.

impair the servers or deprive X Corp. of their use." Order 10. Similarly, X's expenditures of *money* to block or answer undesired server requests do not deprive X of the *servers'* use. *Id.* The Proposed Amendment's injury allegations do not satisfy the Court's criteria. X still fails to identify ***any*** server failure or diminished ability to serve its customers. That is dispositive.[3]

X's Servers Functioned Properly. X does not accuse Bright Data of mounting a denial-of-service attack. Nor does it claim that X lost the use of any of its servers for ***any*** period of time, let alone a "substantial time." *See* Order 9 ("Intermeddling is actionable only if … the possessor is deprived of the use of the chattel for a substantial time."). To the contrary, by admitting that it can't tell the difference between Bright Data's automated requests and individual users' manual requests, X confirms this Court's finding that Bright Data's "scraping tools and services … are reliant on X Corp.'s servers functioning exactly as intended." *Id.*; PSAC ¶ 94.

So, X tries to paint over its deficiencies with internet jargon. But actions that [redacted] or "barrage," "strain" and "tax[]" servers are synonymous with X's prior defective characterizations. X Br. 4-6. A used or even strained, ***but properly functioning***, server is not a failed server. *Id.*; Order 9 (rejecting conclusory statement that "acts have diminished the server capacity"). Recognizing this, X tries to slip the word "failure" into the complaint. But it alleges only that "inauthentic web requests" in aggregate *could* cause X's servers to "fail *more regularly*." X Br. 4 (citing PSAC ¶ 91). The possibility that a server could fail, however, does not mean it *has* failed. Indeed, X's allegation – that it employs a [redacted] that mitigates the risk of [redacted] and "ensure[s] that the system

[3] X questions this Court's holding that automated access is not inherently a trespass injury, saying that Judge Chen suggested otherwise in dicta in *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 n.11 (N.D. Cal. 2017). But, as this Court explained, Judge Chen's footnote referred specifically to "denial of service" attacks, not mere automated access. *Id.* The Ninth Circuit similarly drew the same distinction between "a denial-of-service (DoS) attack," in which "an attacker ***seeks to prevent legitimate users from accessing a targeted computer***," and scraping of "the public parts of [a] website." *hiQ Labs, Inc. v. LinkedIn Corp.,* 31 F. 4th 1180, 1202, & nn. 12, 22 (9th Cir. 2022) (noting that LinkedIn failed to allege that "scraping of ***public profiles*** caused any … technological harm").

overall is less likely to fail entirely" (PSAC ¶ 89) – confirms its ability to manage traffic from *all* website visitors without failure or degradation.[4]

X says, never mind the lack of failed server allegations, look instead at the [redacted] of known data scraping" that its IT Team "responded to and remedied" last year, "where the demands on X's server capacity jumped extreme amounts." *Id.* ¶ 92. But X does not allege that any of these involved Bright Data. Even had it done so, the allegation that "capacity jumped extreme amounts" is just lawyer characterization and not the same as an allegation of server failure. *Id.* Indeed, the fact that X's servers handled this traffic confirms that X was not deprived of their use.

X fares no better in alleging [redacted]. That may speak to the competency of X's IT Team, but it has nothing to do with Bright Data. [redacted] That does not establish any injury caused by data scraping, let alone Bright Data. Nor is X's attempt to use Bright Data as a scapegoat for its inability [redacted]

[redacted] That allegation only addresses the efficacy of X's blocking technology. It says nothing about any deprivation of personal property. As this Court already held, attempts to block access to servers is not a cognizable trespass harm. Order 10.

[4] X's argument that *any* [redacted], regardless of cause, *might* lead to a [redacted] does not save its claim. *See* PSAC ¶ 89. Occasional server failure is an inherent (if undesired) technological property of all servers. Such failures could be caused by any request, whether automated or not. X does not allege that automated requests cause more server failures than manual requests, and thus, cannot show that X's servers failed to function as they ordinarily would in response to any request. In any event, an [redacted] failure is the antithesis of a deprivation for a "substantial" period of time. Order 10.

Unable to identify any server failure, X resorts to a litany of meaningless statistics purporting to show that automated scraping is more voluminous than a *single* human sitting at a keyboard. X Br. 5, 7. But the ***key statistic*** in the Proposed Amendment is the one X ignores in its motion: Only [redacted] PSAC ¶ 87. This allegation kills X's trespass claim because *all* the unauthorized web search – of all kinds, *collectively* (and not just scraping) – is *de minimis*, and far below the [redacted] excess server capacity X maintains to handle such requests. *Id.* ¶ 90.

X's other cherry-picked statistics also do not overcome this fundamental deficiency. For example, X says that scrapers may [redacted] *Id.* ¶ 83. Putting aside the fact that Google is a [redacted] user too when it scrapes X's platform, this is merely an allegation that a scraper is different than an individual user. It is *not* an allegation that, collectively, scrapers make more requests than [redacted] users, let alone an allegation that scrapers – or Bright Data in particular – have degraded X's servers. Nor does this allegation address the Court's observation that "the load placed on the host's server may in fact be *lighter*, because the scraper may only need one web resource, rather than the dozens a web-browser may need." Order 9; Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U.J. Sci. & Tech. 372, 384-85 (2018) ("Courts can also run astray if they start their analysis at what a human sees at the web browser level and work from there to get to the data that scrapers extract, or imagine the scraper as an automaton replicating the steps of a human at a faster rate.").

Recognizing that "apples-to-apples" comparisons between individual and automated access undermines its point, X presents ***misleading*** statistics that <u>*exclude*</u> the most common form of individual access – that is, access through mobile phones. *See* PSAC ¶ 87 (defining "web" access as distinct from iOS/Android, and noting that the "numbers below refer [only] to web traffic"). This tactic may inflate its statistics, but it also renders them meaningless. X does not allege that its server capacity depends on the type of device used to access X's site, whether desktop, laptop, or phone. For the same reason, X's allegation that individuals and scrapers may be interested in different content is irrelevant. An "ordinary" user, X says, may be more interested in "popular" tweets, while scrapers may be interested in other things too. *Id.* ¶ 83. But X chose to make all that information available, and has established a server infrastructure to efficiently deliver the content. X's lawyer characterization that it is "far more burdensome" to display unpopular tweets than popular ones is neither a well-pled fact nor remotely relevant. *Id.*[5]

X's Investment in Server Capacity Is Not a Trespass Harm. With no server failure to speak of, X falls back on the money it spends to operate its platform, including investments in: (i) general operation; (ii) anti-scraping technology; and (iii) extra server capacity.

The first two are easily dispatched. X's allegation that it spent "billions of dollars" to create a "Recommendation Algorithm," for example, has nothing to do with automated access or the deprivation of personal *property*. PSAC ¶ 81. And X's allegation that it "suffers harm even in attempting to impose technological measures to stop data scrapers," and its allegations detailing those efforts, directly contradict this Court's admonition to "keep … in mind" that the "time and money spent attempting to restrict access cannot be bootstrapped into an injury to [a plaintiff's] possessory interest in its computers." *Id.* ¶¶ 90-94; Order 10 (citing *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1359 (2003)).

That just leaves the third bucket: investment in server capacity. This too is no trespass injury. Specifically, X alleges that it "spend[s] [redacted] to ensure that its service remains responsive to actual users." PSAC ¶ 82. But the vast majority of this cost has nothing to do with scrapers, and even less to do with Bright Data. X invests in server capacity for many reasons. If it did not, it wouldn't have a service at all.

Recognizing this, X focuses on the [redacted] per month it allegedly spends purchasing [redacted] to handle unwanted automated server requests. X Br. 4; PSAC ¶¶ 90-91. In X's view, if it buys just one "extra" server, it can enjoin every scraper in the world for all time. The law of trespass does not work that way. Just as spending money to *prevent* a trespass is not trespass harm, spending money on infrastructure to *acquire* property that then

[5] For example, X alleges that scrapers disproportionally account for *certain* types of requests, such as [redacted] for [redacted] PSAC ¶ 87. But it does not matter that individuals account for [redacted] of requests for Elon Musk's tweets, and scrapers account for [redacted] of the requests for his public profile info. As X explained, it developed its [redacted] works as intended for both types of requests. *Id.* ¶ 89.

functions *as intended* is not trespass harm. The law of trespass focuses only on the deprivation of plaintiff's property, not the *reasons* the plaintiff acquired the property in the first place. A person, for example, cannot buy an answering machine for their landline to screen calls, and charge that cost back to the telemarketer by claiming it was deprived of the use of the answering machine. The answering machine worked as intended, so there was no deprivation of its use. So too, there is no *deprivation* of the extra server capacity X purchased to handle automated server requests. Put simply, if X wants to complain about its expenditure of money, trespass is not the right tort.

X's reliance on its investment in extra server capacity fails for the additional reason that the supposed injury does not flow from the *completed* trespass, but from the future, post-acquisition risk of it. As the California Supreme Court recognized in rejecting the "bootstrapping" of infrastructure costs to address the risk of future trespasses, "injury can only be established by the completed tort's consequences." *Intel*, 30 Cal. 4th at 1359. Under *Intel*, a trespass harm is one that *follows* the trespass, not a cost incurred in anticipation of it. X does not allege that it spent a penny *following* a supposed trespass by Bright Data.

2. *X's Access Claims Fail for the Additional Reasons Raised in Bright Data's Original Motion to Dismiss.*

The Court not only required X to address its deficient injury allegations; it also required X to "demonstrate how the proposed amended complaint corrects … all other deficiencies raised in Bright's Data's motion." Order 26. The Proposed Amendment does not do this. As Bright Data previously explained, X's trespass claim fails because (i) X consented to or assumed the risk of unwanted server requests when it connected to the Internet; and (ii) it alleges only that Bright Data intended to communicate with X's servers, not to degrade or impair them. X's Proposed Amendment adds ***no new facts*** addressing either deficiency. It just re-argues the law. A Motion to Amend, however, is not an invitation to redo the briefing on the same facts, claims, and legal theories. *See Bonin v. Calderon*, 59 F.3d 815, 845 (9th Cir. 1995) ("a district court does not abuse its discretion in denying a motion to amend where the movant presents no new facts"); *Nunes v. Ashcroft*, 375 F.3d 805, 808 (9th Cir. 2004) (same); *Cox v. CoinMarketCap OPCO, LLC*, 2024

WL 3748982, *11 (9th Cir. 2024) (same). But even if the Court were to consider these issues anew, X's arguments fare no better now than before.

i. X Consented to or Assumed the Risk of Automated Access When it Connected to the Internet.

As this Court explained, the "exchange of information across another's internet-connected system is to be expected," and indeed, the "internet was designed to enable this exchange." Order 8. For that reason, an automated request for information made *for the purpose of communicating* with another internet connected device is not a trespass.

When X connected its servers to the Internet, it joined hundreds of millions of people who also enjoy the right (and obligation) to send and receive communications through the network, according to standard Internet Protocols. Having voluntarily chosen to participate in the world wide web, X cannot impose liability on those who are likewise using the web for communications purposes. Under California law, when a person participates in a group activity – whether a sports event or a global communications network – any ensuing contact will not constitute a trespass unless it is "***totally outside the range of the ordinary activity*** involved" in the endeavor. *Knight v. Jewett*, 3 Cal. 4th 296, 320 (1992).

As this Court noted, whether some types of automated access "support a claim for relief is … contextual." Order 8. From this, X posits that any server request is a trespass if the sender was aware that it was unwanted. But that is not the rule. As one commentator explained,

> "While one might assert that an unwanted HTTP request is a real property trespass, … this doesn't make sense. [It] is similar to my picking up the telephone to find that there's a solicitor on the other end…. I hardly have a cause of action for real property trespass if the solicitor starts to talk."

See Eric Feigin, *Architecture of Consent: Internet Protocols and Their Legal Implication*, 56 Stan. L. Rev. 901, 931 (2004). Rather, the correct rule focuses on whether the request is "totally outside range of ordinary" internet usage. *Knight*, 3 Cal. 4th at 320.

This rule emanates from two separate, but related, principles. *First*, the act of participating in the activity is itself consent for any contact normally associated with it. *See* Rest. 2d Torts, §§ 49, 50, 892(a) cmt. a ("No one suffers a legal wrong as the result of an act to which…he freely consents or to which he manifests apparent conduct."); *Price v. Apple, Inc.*, 2022 WL 1032472, *6 (N.D. Cal. 2022) ("consent dooms [a] trespass claim."). *Second*, when contact is "inherent in the activity" – such as tackling in football or the sending and receiving of electrons via the web – all participants have assumed the risk that some unwanted contact may occur. *Knight*, 3 Cal. 4th at 311; *see* Rest. 2d Torts, § 50, cmt. b ("Taking part in a game manifests a willingness to submit to such bodily contacts or restrictions of liberty as are permitted by its rules or *usages*."); *id*. § 53, cmt. a (same).[6]

X ultimately concedes that it must show that Bright Data's conduct is "outside the range of the ordinary activity." X Br. 2 (citing *Knight*). It asks this Court to rule – *as a matter of law* – that automated server requests made for the purpose of exchanging information fall "totally outside" that range. But that would require this Court to find that automated access is outrageous conduct, even though entire industries are built upon such access, including web search engines, price comparison ecommerce sites, and the entire growing field of A.I. The Court cannot do that. Indeed, X itself admits that automated access and scraping is perfectly legitimate. It not only allows, but wants, Google to scrape its platform and display the results in Google's search engine to enhance X's popularity. PSAC ¶¶ 64, 75. Certainly, if X permits scraping by some, it is not "totally outside the range of ordinary activity" when others, like Bright Data, engage in exactly the same conduct.

X's only argument is that its Terms give it total control over who may send a server request. But it does not matter what X's Terms say. X's Terms are not the *source* of consent; its connection to the Internet is. X cannot negate that consent by declaring unwanted requests verboten. A football player, for example, is not the victim of a tort if he is tackled while wearing a jersey that says, "don't mess with me." If he doesn't like the rules, he can pick up his football and go home,

[6] X does not allege any violation of any Internet Protocols. Even if it had, a violation of some rule is not enough to place the conduct outside the "range of ordinary activity." *See Hunt v. Zuffa, LLC*, 361 F. Supp. 3d 992, 1009 (D. Nev. 2019) (no liability for physical injuries enhanced by illegal steroid use; "By "enter[ing] a sport," the player has "consent[ed] to physical contacts" within "the range of ordinary activity" associated with the endeavor, and other participants do not "exceed[] the scope of … consent" just because the contact constitutes a rules violation); *Avila v. Citrus Cmty. Coll. Dist.*, 38 Cal. 4th 148, 152 (Cal. 2006) (no liability for baseball "beanball[s]"); Rest. 2d Torts § 50, cmt. b (no liability for tackling an opponent while "offsides").

but he can't impose his own rules over the objections of the other participants who just want to play the game. The reason is simple. If the player wants to enjoy the benefits of playing the game with others, he has to consent to, or assume the risks of, contacts normally associated with it.

That is not to say that X is powerless to prevent truly malicious conduct, such as phishing, DoS attacks, or password hacking, since that conduct is "totally outside the range of the ordinary activity" associated with internet communications. *Knight*, 3 Cal. 4th at 320. But mere automated access is not.[7] Indeed, giving X the unbridled power it now seeks is subject to its own abuses. Just imagine if X were to insert a provision in its Terms that prohibited anyone whose name begins with an "A" from accessing its site. Would everyone from **Alice to Alsup** now be liable in trespass for typing www.X.com into their web browser? No. That is not for lack of injury, but because the law of trespass does not make search for purposes of *ordinary* communications illegal.

X misplaces reliance on *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000). Putting aside the fact that the California Supreme Court disagreed with *eBay* in *Intel*, 30 Cal. 4th at 1357, *eBay* was an early foray into cyberspace communications at the dawn of the Internet Age when scraping was a relatively new phenomenon. The court tried to draw analogies to physical trespass cases, which are simply inapt in the digital world. While it did the best it could, the court failed to appreciate the central fact that the Internet itself is a global communications *network*. As such, it failed to consider whether eBay provided the requisite consent when connecting its servers to the Internet.

Nor did the *eBay* court have the benefit of the Ninth Circuit's decision in *hiQ*, 31 F. 4th 1180, 1202 (9th Cir. 2022), and thus, *unlike this Court*, did not "carefully consider[] each of the claims asserted" in light of the Ninth Circuit's concerns about the "creation of information monopolies." *See* Order 2. By assuming incorrectly that eBay's Terms were the *only* source of consent, the court effectively allocated all the power to dictate usage to the website operator, without due regard for those on the other end of the line. That was wrong. As this Court rightly

[7] *Civic W. Corp. v. Zila Indus., Inc.*, 66 Cal. App. 3d 1, 17 (1977), is inapposite. It involved trespass to real property, no group endeavor, and outrageous conduct, including "ejecting [debtor]'s employees and changing the locks on the doors."

recognized, X is seeking to use its Terms to create a monopoly over data it does not own and that is otherwise freely and publicly available, solely for the purpose of blocking competition for the sale of such data. The Court should decline the invitation to use common law trespass to chattels to create such monopolies.

ii. X Fails to Allege <u>Intentional</u> Interference with Its Property.

X's trespass claim also fails because it has not alleged that Bright Data intended to deprive X of use of its servers, or knew that its conduct was "certain or substantially certain" to have that effect. *See* Rest. 2d Torts, § 8A, cmt. a ("Intent … has reference to the consequences of an act rather than the act itself."); § 217, cmt. c ("Intention is present when an act is done for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a ***substantial certainty***, result from the act.").

People touch others' property every day. A janitor, for example, may intentionally pick up a book left on a table, and place on a shelf. But there is no intentional trespass, even though he did so knowingly and the book's owner was, in fact, deprived of its use until the book was found. Why? Because there was no intent to deprive the owner of its property.

Here, too, sending server requests to X's servers – knowing that X has server farms capable of handling these requests as they come – is not an intentional trespass. As this Court recognized, Bright Data's "scraping tools and services … are reliant on X's Corp.'s services functioning exactly as intended." Order 9 (citing *WhatsApp, Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 684-85 (N.D. Cal. 2020)). This is the opposite of an intent to engage in activity that deprives X of the use of its platform. As Judge Oliver Wendell Holmes famously said, "even a dog knows the difference between being kicked and being stumbled over." That principle applies here too. Using the Internet to communicate is what the Internet is for, so sending server requests for that purpose does not cause *deliberate* injury. For that reason, X's trespass claim fails.

B. X's Amendment to its Fraud and Unfair UCL Claims Is Futile.

This Court dismissed X's UCL claim because X failed to allege any "unfair business act … beyond [the] bare recitation of the word unfair," any violation of a "predicate claim," or any misrepresentation. Order 11. In seeking to resurrect that claim, X presents no new facts.[8] Instead, it re-argues its failed contention that scraping is inherently "immoral, unethical, oppressive, unscrupulous[,] or substantially injurious to consumers." X Br. 9. But this Court already rejected that argument, which is now law of the case. Even if it were not, as Bright Data previously explained, in competitor lawsuits, courts construe the "unfair business act" prong consistently with the antitrust laws. ECF 49 at 24. X does not attempt to satisfy that standard.

X's attempt to resurrect its failed fraud-based claim also falls short. As an initial matter, X does not attempt to resurrect its UCL fraud claim for any alleged ***public scraping***. So leave to amend the complaint to bring a public scraping UCL fraud claim should be denied.

Instead, X now tries its hand at bringing a UCL fraud claim based on speculation that Bright Data may have scraped behind a log-in screen. That allegation is not plausibly pled. X still does not dispute that "[t]hose who do not register for accounts on X can still access the platform." Order 2. Nor has it identified any scraped data that "is solely accessible to X users logged in to registered accounts or was otherwise password-protected." *Id.* at 4. To the contrary, X continues to admit, as it must, that significant amounts of "X user content … is publicly accessible on the user side of the X platform," including "information relating to [a] user's specific geographical locations," "number of likes, replies, and reposts," and that such content is "available to individuals who are not logged in." *See* PSAC ¶¶ 50, 64-65. Indeed, X goes further, admitting that because it has given Google free reign to "crawl" all of X's publicly available content, any content that appears in "Google's search results" is publicly accessible without a login. *Id.*

The Proposed Amendment also fails to identify ***any*** information that Bright Data scrapes that is behind a log-in.[9] At best, X says there is some "*other* content" that may not be publicly available, and that logged-in users can do things non-registered users cannot. PSAC ¶ 66. For

[8] X also cites its new claims as "predicate claims." Since Bright Data will address the deficiencies with the new claims on a post-amendment 12(b)(6) motion, it will also, if necessary, address the "predicate claim" prong of the UCL at that time as well.

[9] In its Motion, X mischaracterizes its own complaint, saying that it "clarifies that much of the data Bright Data and its customers scrapes is not available to the public." X Br. 9 (citing PSAC ¶¶ 25-28, 64-70). Just reading those paragraphs reveals the lie.

example, X alleges that registered users have "full" access to the platform, and can "post and share" content. *Id.* ¶¶ 24-25. But scraping does not involve posting or sharing content, and "full" access is not required for scrapers to access, view, or copy public content. Nor is it relevant that *some* data is private, since X does not allege that ***any*** of that content was scraped.

X's only retort is to says it is "dubious[]" that all Bright Data's "datasets sourced from X contain only publicly accessible data." *See Id.* ¶ 120. But X's skepticism is not a factual allegation. As this Court observed, Bright Data's product descriptions – as alleged in the Complaint – all make clear that its datasets and scraping tools are limited to public information. Order 4. The Proposed Amendment continues to focus on the same tools, with the same descriptions.[10] X does not allege that any of these product descriptions are false.

Instead, it says that it would be hard collect the *volume* – not type – of information Bright Data scrapes without using "legions of fake accounts." PSAC ¶ 79. But it does not actually allege that Bright Data used any account (fake or otherwise) for purposes of automated access or scraping. Rather, it just alleges that the "only feasible means of data scraping the limited content that is accessible to non-logged-in users is by circumventing X's ***IP rate limits*** and ***anomaly-detection tools***." *Id.* ¶ 69. Avoiding rate limits is not the same as using a fake account. Nor can X overcome its pleading hurdle by rhetorically invoking this Court's hypothetical, where a person who, after being terminated, engages in some misrepresentation in signing up for a second account. X Br. 9. X has not alleged any misrepresentation that Bright Data engaged in connection with any account creation. These omissions are fatal because a plaintiff must allege its fraud-based UCL claim with ***particularity***, under Rule 9(b). *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126-27 (9th Cir. 2009) (UCL claims "grounded in fraud" "must be ple[d] with particularity").

[10] X claims that Bright Data's underlying proxy infrastructure (but not its scraping tools or datasets) could theoretically be used for logged-in access because a proxy network – like a basic broadband connection – is just an intermediate internet connection. PSAC ¶ 122. But X specifically admits that Bright Data employs a process called, "Know Your Customer," to prevent such usage. *Id.* X's argument that this process is a "sham" is conclusory, and not a well-pled allegation. *Id.* Indeed, its only support for its conclusory allegation is the fact that Bright Data offers *public* datasets for sale. *Id.* Its argument is a non-sequitur.

In fact, even under Rule 8, X pleads itself out of court because it expressly alleges "an obvious alternative explanation" of how X's site can be scraped at scale without an account. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 567 (2007). This can be achieved, it says, using Bright Data's "72 million" "rotating IP addresses," which would enable a scraper to access X's servers while "appear[ing] as if it were a regular human user," making it "nearly impossible" to block. PSAC ¶¶ 79, 93, 129, 132. X presents no facts – ***zero*** – why fake accounts would still be needed in that instance to scrape X's *public* sites. Thus, X's speculation that Bright Data may be using fake accounts is just a logically-flawed lawyer's *conclusion* drawn from facts that are, at most *possibly* consistent with, but certainly not suggestive of, illegality. *Twombly*, 550 U.S. at 557 ("The need at the pleading stage for allegations plausibly suggesting (***not merely consistent with***) [illegality] reflects the threshold requirement [that the Complaint] possess enough heft to 'show that the pleader is entitled to relief.'").

C. X's Amendment to its Contract-Based Access Claims Is Futile.

This Court dismissed X's contract and tortious interference claims because X failed to allege "damage resulting from automated access to [its] systems." Order 15.[11] As the Court explained, "merely alluding to diminished [server] capacity and reputational harm, without pleading any impairment or deprivation of servers" is not sufficient. *Id.* at 17. Conceding that it is largely relying on the same "types of injuries" for both its trespass and contract claims, its injury allegations fail for the reasons "outlined above." X Br. 8. X's only new argument is that its contract damages extend beyond server impairment and include lost sales of its own competing datasets. *Id.* But such speculation is not an injury from automated *access*, as opposed to scraping.

[11] X argues that the Court "ruled that Bright Data is bound by the Terms" because it was aware of the terms. X Br. 8 (citing Order 15-17). But the Court did not, and could not, address the issue of rejection, which was raised only by Bright Data's Summary Judgment motion based on unpled facts. Nonetheless, in finding X's post-complaint amendments to the terms ineffective, the Court implicitly agreed that the Terms can be rejected. Order 25-26. The reason is not because there is something magical about a court proceeding, but because the act of litigation manifests rejection of any post-suit offer. *Id.* (citing *Al-Safin v. Cir. City Stores, Inc.*, 394 F.3d 1254, 1260 n.5 (9th Cir. 2005) (noting that post-complaint contract amendments are just "*offers*.").

Indeed, X's Terms expressly permit automated *access* to X's site. PSAC ¶ 30 (defining an access misuse *only* as "access …other than through … currently available, published interfaces").[12]

For these reasons, X's Proposed Amendment to its Access Claims is futile.

III. X'S AMENDMENTS TO ITS PRIOR SCRAPING CLAIMS ARE FUTILE.

A. The Court Should Decline to Revisit Its Preemption Ruling.

This Court held that, "to the extent X Corp.'s state-law claims are based on scraping and selling of data," "they are preempted" by the Copyright Act. Order 25. X now seeks to revive its claims because it "respectfully disagrees with the Court's preemption ruling." X Br. 10. But the Court did not invite X to amend the preempted claims. X simply seeks reconsideration of a legal issue the Court already decided. A motion to amend is not the proper vehicle for that. *Cox*, 2024 WL 3748982, at *11. But even if it was, X alleges no new facts bearing on the preemption analysis, just an extended manifesto as to why it believes scraping is bad. These are policy arguments, not factual allegations. Nor does X's sophistry undermine this Court's prior holding. Where, as here, a claim's "defects lie in the legal theories … any amendment would be futile."[13] *Saloojas, Inc. v. United Healthcare Ins. Co.*, 2023 WL 7393016, *4 (N.D. Cal. 2023) (Alsup, J.). The Court should summarily deny the motion to amend the Scraping Claims.

B. X's Scraping Claims Conflict with the Copyright Act.

Even if the Court were to consider X's Scraping Claims afresh, it would still find them preempted. As this Court previously explained,

> "The upshot is that, invoking state contract and tort law, X Corp. would entrench its own private copyright system that rivals, and even conflicts with, the actual copyright system enacted by Congress. X Corp. would yank into its private domain and hold for sale information open to all, exercising a copyright owner's right to exclude where it has no such right…. [This] massive regime of adhesive terms

[12] Indeed, the consequential damages X alleges are, at most, an indirect derivative injury. Such damages are not cognizable because they are (i) not proximate, as they depend on the hypothetical conversion of scrapers to X data customers, and (ii) preempted, as they are based on scraping.

[13] *See Epikhin v. Game Insight N. Am.*, 2015 WL 2412357, *6 (N.D. Cal. 2015) (denying "leave to amend because [the claim] is preempted by federal law and amendment would therefore be futile"); *Velazquez v. David*, 2014 WL 11515023, *2 (C.D. Cal. 2014) ("Because all the claims are preempted by Section 301," dismissal is "without leave to amend."); *Schuler v. Medtronic, Inc.*, 2014 WL 988516, *1-2 (C.D. Cal. 2014) (same).

> imposed by X Corp. … stands to fundamentally alter the rights and privileges of the world at large." Order 20.

X's Motion does not grapple with the Court's concern. It does not dispute that it seeks to use state law to block the reproduction and sale of information that it either does not own or that Congress has affirmatively made freely available for public use. Order 23-24. Instead, it argues that this poses no threat to the Copyright Act and serves a variety of made-up state interests. It is wrong.

1. ***X's Claims Conflict with the Purposes of the Copyright Act.***

X says there is no conflict with the Copyright Act because X wants to use state law to prevent scraping of data that it does not own, or that the Constitution places beyond Congress's power to act. Neither argument has merit.

Enforcement of State Law to Prevent Scraping of Users' Content Conflicts with the Act. As to user-generated content, X tries to avoid preemption by "now disclaim[ing] any attempt to enforce X's users' copyrights." X Br. 12; PSAC ¶ 42. Putting aside the fact that X's use of the word "now" is misleading because X *never* tried to enforce users' copyrights, its disclaimer is of no moment. As Bright Data previously explained, "X's argument – that it can avoid preemption because it 'does not own' the information – turns Copyright law on its head. By granting exclusive rights to copyright holders, the Act ***extinguishes*** third-party rights. X cannot gain rights to that same information by disclaiming ownership in it." ECF 70 at 9. To allow such a suit would transform rights exclusively vested in the content *creator* into a non-exclusive right co-controlled by the content distributor. Congress did not permit that. *See ML Genius Holdings LLC v. Google LLC*, 2022 WL 710744, *4 (2d Cir. 2022) (state law claims relating to scraping of song lyrics owned by others preempted).

Nor is it any answer to say that users still have their exclusive *federal* rights because X is suing under state law, not copyright. That is true in all preemption cases. As this Court recognized, preemption prevents the creation of a dual legal regime under state law that "rivals, [and] even conflicts with, the actual copyright system enacted by Congress." Order 20. That X is not suing under copyright is the problem, not the solution.

X next says that it is not creating a rival system because it is just using contract law to achieve its ends. Borrowing a page from express preemption, X says contract law can't conflict with copyright because it has "extra elements" of promise and consideration. But as Bright Data previously explained, the majority of courts ***reject*** the argument that contract claims cannot be preempted. ECF 70 at 11-12 (citing cases); *see also* Order 22 n.6 (it is "prudent to refrain from adopting a rule that anything with the label 'contract' is necessarily outside the express preemption clause.") (citing *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1455 (7th Cir. 1996)).[14] X does not grapple with this case law. Instead, it cites the same minority view Bright Data previously addressed, largely involving information "use," not its reproduction and sale.[15] X Br. 11.

X's cite to *Grosso v. Miramax Film Corp.*, 383 F.3d 965 (9th Cir. 2004), confirms that using contract law to *prohibit copying* conflicts with the Copyright Act. There, the plaintiff sought to enforce a "*promise to pay*" for content. A "promise to pay" and a "promise not to copy" are not the same. As the Second Circuit explained, "not all 'extra elements' are sufficient to remove the claim from the 'general scope' of copyright." *Genius*, 2022 WL 710744, at *3. An extra element will not save a contract claim from preemption "if it is merely based on allegations that the defendant did something that the copyright laws reserve exclusively," such as "unauthorized reproduction, performance, distribution, or display." *American Movie Classics Co. v. Turner Enter. Co.*, 922 F. Supp. 926, 931 (S.D.N.Y. 1996); *see also* Nimmer on Copyright, § 1.14(C) (2023) (similar). This explains why a "promise to pay" and a "promise not to copy" are treated

[14] *Wrench LLC v. Taco Bell Corp.*, 256 F.3d 446, 457 (6th Cir. 2001) ("We do not embrace the proposition that all state law contract claims survive preemption simply because they involve the additional element of promise."); *Genius*, 2022 WL 710744, at *4 ("a per se rule that all breach of contract claims are exempt from preemption … would be in tension with our precedent."); *Ritchie v. Williams*, 395 F.3d 283, 287 (6th Cir. 2005) (preempting claims relating to a "partnership agreement" designed to "control the ownership, performance rights and exploitation of copyrights on songs written by Kid Rock."); *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255, 270 (5th Cir. 1988) (breach of license agreement preempted); *Kabehie v. Zoland*, 102 Cal. App. 4th 513, 525 (2002) ("while "[a] few courts have concluded that breach of contract actions are never preempted … because the promise to perform … automatically constitutes the extra element," those "courts are in the distinct minority.").

[15] *Compare* X Br. 11-12 & n.2 (citing *Altera*, *Blizzard*, *Bowers*, *Nat'l Car Rental*, *ProCD*, and *Craigslist*), with ECF 70 at 11-12 & n.8 (addressing the same cases).

differently. While an agreement to ***allow*** copying may provide *consideration* for a promise to pay for it, the action to recover a debt owed is not an action to *prevent* the permitted copying.[16] A suit to ban scraping, in contrast, is a suit to prevent copying. That is why it is preempted.

But even if X's state law claims involved extra elements, it does not avoid preemption. It only kicks the analysis from express preemption into implied preemption.

> "Although conflict preemption has played second fiddle to express preemption in the caselaw as of late, it is the more appropriate consideration when the question presented is not whether *rights* created by state law are *equivalent* to rights created by federal copyright law but whether *enforcement undermines* federal copyright law." Order 21.

X's response – that Bright Data is too small or too sophisticated to "imperil … federal objectives," *see* X Br. 12 – is a non-sequitur. Bright Data's size and sophistication are irrelevant. X's attempt to assert control over data it does not own – and to use state law to block copying when the Copyright Act exclusively vests those rights elsewhere – imperils the federal copyright scheme.

For the same reason, there is no merit to X's disclaimer that it is not seeking to "obliterate" the Copyright Act's "fair use" exception. X Br. 14. In X's view, there is no conflict with federal law because Bright Data could still "invok[e] fair use as a defense" in some "future" copyright suit. X Br. 14.[17] But this misses the point. In establishing the fair use exception, Congress determined what information should be freely available for public use. Using state law to strip the public's right to use such information conflicts with the Act. Indeed, the fact that the "fair use" exception is not a defense to the state law claims proves that the state law claims are in conflict.

[16] *Grosso* involved an "implied-in-fact" contract, meaning that there was a contract to allow the use of the plaintiff's information. 383 F.3d 965. This differs from an implied-in-law contract in which the contract is just a legal fiction. In expressly limiting *Grosso*, the Ninth Circuit held that "implied-in-law" contracts, such as claims for unjust enrichment, do not involve extra elements. *Best Carpet Values, Inc. v. Google, LLC*, 90 F.4th 962, 974 (9th Cir. 2024).

[17] X misplaces reliance on *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005). There, the defendant reverse engineered the plaintiffs' source code, which involved incidental copying and further "*use*" of the information. The court held the defendants' contractual waiver of a "fair use" defense was effective. But waiver of a federal defense is a federal, not state, law question, so preemption is irrelevant. Preemption also did not apply to the subsequent "*use*" of the code, because unlike copying (or scraping), use is not an exclusive copyright right.

Enforcement of State Law to Prevent Scraping of Facts Conflicts With the Act. X concedes that all the data it *owns* is not copyrightable. It says this saves its state law claims from preemption. The opposite is true.

X does not dispute that express preemption extends to the "general scope" of copyright, and to non-copyrightable information, such as facts and figures drawn from larger copyrightable works. ECF 60 at 5-7 (citing cases).[18] As the Ninth Circuit held, "[a] work need not consist *entirely* of copyrightable material in order to meet the subject matter requirement." *Best Carpet*, 90 F.4th at 971. Because X's site is indisputably copyrightable (PSAC ¶ 190), preemption applies even to the site's non-copyrightable elements. X neither takes issue with this principle nor claims that it is limited to express preemption. Indeed, both preemption doctrines prevent States from encroaching on Congress's demarcation of the respective rights of authors and audiences.

Instead, X says that Congress didn't really make any such determination that facts and figures should be in the public domain because it was constitutionally *prohibited* from doing so. In X's view, States are the *exclusive* sovereign with the power to regulate dissemination of facts and figures. X cites no authority for that proposition. And were it so, the legion of cases that find preemption over non-copyrightable content would all be wrong. Nor is the fact that Congress chose not to protect factual information evidence of its incapacity to place it in the public domain. As the Supreme Court explained, "where the need for free and unrestricted distribution of a writing is thought to be required by the national interest, the Copyright Clause and the Commerce Clause would allow Congress to eschew all protection. In such [a case], a conflict would develop if a

[18] *Genius*, 2022 WL 710744, at *2 (rejecting argument that preemption does not apply to non-copyrightable "transcriptions" because "section 301 prevents the States from protecting [a work] even if it fails to achieve Federal statutory copyright [for lack of] originality."); *Ticketmaster Corp. v. Tickets.Com, Inc.*, 2000 WL 525390, *4 (C.D. Cal. 2000) (dismissing misappropriation and trespass claim because, "[t]o the extent that state law would allow protection of factual data (not clear at all), this cannot be squared with the Copyright Act."); *Harper & Row Publishers, Inc. v. Nation Enters.*, 723 F.2d 195, 200, 208 (2d Cir. 1983), *rev'd on other grounds*, 471 U.S. 539 (1985) (claims involving copying of "essentially factual" information from President Ford's memoirs preempted); *Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841, 850 (2d Cir. 1997) (same); *Barclays Cap. Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876, 892 (2d Cir. 2011) (same).

State attempted to protect that which Congress intended to be free from restraint." *Goldstein v. California*, 412 U.S. 546, 559 (1973).[19]

2. *X Cannot Avoid Preemption By Disparaging Scraping.*

X tries to avoid preemption by presenting a litany of arguments as to why scraping is bad, suggesting that California has an *overriding* interest in banning the practice. But California did not ban scraping. And the three interests X cites have nothing to do with the state laws it invokes.

First, X invokes a *user's* privacy interests. But X lacks standing to sue to protect user privacy. As this Court recognized, X's interest in "protect[ing] X users' privacy" evaporates "so long as it gets paid." Order 25. In any event, this case does not concern private information. It concerns public information. As one court explained,

> "A tweet from a user with public privacy settings is just a twenty-first century equivalent of an attempt to publish an opinion piece or commentary in the New York Times…. [T]here can be ***no reasonable expectation of privacy***."

Rosario v. Clark Cnty. School Dist., 2013 WL 3679375, *5 (D. Nev. 2013).[20] Nor does X's anti-scraping technology transform public information into private. Even if X's rate limiters effectively blocked all third-party scraping, users' public posts do not magically become "private" when X sells the same data through its API service, or when X allows Google to scrape the information to display on the most popular search engine in the world. X's only retort is that it believes it does a better job protecting user privacy than Bright Data. But preemption does not turn on whether X's privacy practices are better or worse than Bright Data's. State law does not create a presumption that social media titans are better stewards of user data than those who compete with X in the private marketplace.

[19] X does not address Congress's Commerce Clause authority, which provides a basis for protecting pure facts and figures even separate from broader copyrightable works. *U.S. v. Martignon*, 492 F.3d 140, 152 (2d Cir. 2007) (noting alternative grounds for authority).

[20] *ACLU v. Clearview AI, Inc.*, 2021 Ill. Cir. LEXIS 292 (Ill. Cir. 2021), is not to the contrary. *ACLU* did not involve preemption or copyright. There, state law *created* a property right in biometric information, the definition of which encompassed information *derived* from public photographs. X cites no state law creating a property right in public social media data.

Even putting that aside, the state laws X invokes were not designed to protect user privacy. Contract law is designed to protect bilateral promises, not privacy. Indeed, contract law takes no special interest in the subject matter of the contract. The State's interest in a contract for the delivery of champagne, for example, is not to promote drinking, but to ensure that every person's word is their bond. So too, tortious interference protects the sanctity of contract, not privacy. Misappropriation and unjust enrichment law are designed to prevent the misappropriation of the *plaintiff's* property – they are property protection laws, not privacy protection statutes. Recognizing that ***none*** of its state law claims address privacy, X invokes the California Consumer Privacy Act. X Br. 16. But X has not brought a claim under the CCPA. So, the California legislature's interests in passing the CCPA cannot save non-CCPA claims from preemption. To the contrary, that X felt the need to invoke the CCPA shows that the laws X sued under were designed for *different* purposes.

Second, X argues that its "state law claims also promote … data security." X Br. 17. But, again, none of the previously-asserted state law claims were designed to protect data security. X does not contend otherwise. Instead, it says its own motivation for preventing scraping is not to protect its revenue streams, but to enhance data security.[21] This Court already rejected that argument (Order 25), and it is inconsistent with X's claimed injury, which is based on lost revenues from sales of competing data. PSAC ¶ 48; X Br. 8. X's "assertion that the scraping alleged here violates [users'] 'safety and security' in … publicly disseminated tweets is therefore a non-starter." *X Corp. v. Ctr. for Countering Digital Hate, Inc.*, 2024 WL 1246318, *21 (N.D. Cal. 2024).

More importantly, however, preemption does not turn on the plaintiff's interests; it turns on the *State's* interests in enacting or enforcing the law. And data security was surely the furthest thing from the State's mind when these laws – some of which have their origins in medieval times – arose. But even if X could equate its interests with those of the California legislature, it would do no good. The claims at issue here concern the reproduction and sale of data, as distinct from

[21] X complains that Bright Data "appears willing to sell scraped data to anyone, anywhere, for any purpose." X Br. 18. But X claims it too is willing to sell the same data (and *even more*) to anyone, anywhere, for any purpose. PSAC ¶ 39-50. Indeed, nothing prevents X from, as ***it says***, secretly "selling [the same data] to terrorists or other bad actors." X Br. 18.

X's Access Claims. Thus, even if the State had a substantial interest in preventing unauthorized access to X's platform for data security purposes, that would only address whether the *Access Claims* were preempted, not whether the *Scraping Claims* were.

Third, X claims that Bright Data's scraping undermines "consumer-protection interests." X Br. 19. But scraping is not anti-consumer. It benefits consumers by making public information available to them in a structured, more usable format. More information is not anti-consumer; it is pro-consumer. X does not allege that Bright Data falsified user data, or otherwise deceived any consumer. It simply alleges that Bright Data copied and sold public data. If California's legislature believed that was anti-consumer, they would have passed a law saying so. Nor can X create a substantial state interest by imagining a parade of horribles, like "misleading advertisements, spam, or phishing." *Id.* X does not accuse Bright Data of doing any of that. Nor are allegations about such activities "elements" of the state law claims X asserts. As it stands, X is seeking to prevent the reproduction and sale of public data. California's consumer protection laws do not ban that practice, and if it did, it would conflict with the Copyright Act.

C. X's Scraping Claims are Expressly Preempted.

As Bright Data previously explained, X's Scraping Claims are expressly preempted because they fall "within the subject matter of copyright" and involve rights "equivalent" to the exclusive rights protected by copyright law. *Best Carpet*, 90 F. 4th at 970-71. X does not address express preemption, other than to incorrectly state that the Court found express preemption to be inapplicable. X Br. 9-10. The Court, however, did not find express preemption inapplicable; it decided the case on implied preemption grounds. Express preemption, however, also applies for the same reasons above. Because scraping is *just* the reproduction of data, X's Scraping Claims are equivalent to exclusive copyright rights. Thus, this Court should also find, for purposes of any appeal X may pursue, that X's Scraping Claims are expressly preempted.

D. X's Unjust Enrichment and Misappropriation Claims Fail Because X Does Not Own the Internet.

Even if X's Scraping Claims are not preempted, its proposed amendments to its unjust enrichment and misappropriation claims are futile because X seeks to enforce rights over data it does not own. As Bright Data explained in its prior motion, X's claims fail because it does not have an independent property right to prevent Bright Data from searching and making use of the public web. ECF 42 at 19-22 (unjust enrichment), 29-31 (misappropriation); *see also* ECF 49 at 16-17, 20-23. Indeed, if Bright Data has "misappropriated" X's property, then every business that has looked up information on the Internet has "misappropriated" information the website operator posted to its site.

In response, X concedes that individual search and use of public data is not actionable, but it claims that scraping at scale is. But the law draws no such distinction. The key distinction is whether X has an independent property right that it seeks to enforce, not the volume of data at issue. *See* ECF 49 at 21 (discussing that "under California law … misappropriation … claims are actionable only to vindicate legally protected ***property*** interests") (citing cases). Here, X fails to identify a source of positive law granting it a property right in any data Bright Data scrapes. That dooms its unjust enrichment and misappropriation claims.

But even if X did have a property right in the data, its claims would fail because the California Uniform Trade Secrets Act provides the exclusive state law remedy for the misappropriation of such information. *See* Cal. Civ. Code § 3426; *see Waymo LLC v. Uber Techs., Inc.*, 256 F. Supp. 3d 1059, 1063 (N.D. Cal. 2017) (Alsup, J.) (applying *Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210 (2010) to find that CUTSA superseded Section 17200 claim because "confidential information" did not rise to the level of trade secret and no "other provision of positive law grants a property right in that information"); *Silvaco*, 184 Cal. App. 4th at 239 n.22 ("We emphatically reject the … suggestion that the [CUTSA] was not intended to preempt common law conversion claims based on the taking of information that, though not a trade secret, was nonetheless of value to the claimant…. [A] prime purpose of the law was to sweep away the adopting states' bewildering web of rules and rationales and replace it with a uniform set of principles for determining when one is – and is not – liable for acquiring, disclosing, or using information ... of value.").[22]

[22] *Barker v. Insight Glob., LLC*, 2017 WL 10504692, *4 (N.D. Cal. 2017) ("After *Silvaco*, the majority of district courts have held that CUTSA supersedes claims based on the misappropriation of information that does not satisfy the definition of trade secret under CUTSA.") (collecting

IV. CONCLUSION.

The Court should deny X's Motion to Amend the Complaint for the foregoing reasons.

cases); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 839-40 (N.D. Cal. 2014) (finding CUTSA preempted trespass to chattel and unfair competition claims); *SunPower Corp. v. SolarCity Corp.*, 2012 WL 6160472, *9 (N.D. Cal. 2012) (finding unfair competition and unjust enrichment claims superseded). X's reliance on *Compulife Software Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020), a trade secret case, is inapposite. X has not brought a trade secret claim so any further comparison to *Compulife* stops there.

Dated: August 30, 2024

Respectfully submitted,

/s/ Colin R. Kass

Colin R. Kass*
PROSKAUER ROSE LLP
1001 Pennsylvania Ave., N.W.
Washington, D.C. 20004
(202) 416-6890
ckass@proskauer.com

David A. Munkittrick*
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
(212) 969-3000
dmunkittrick@proskauer.com

Robert C. Goodman (Bar No. 111554)
Lauren Kramer Sujeeth (Bar No. 259821)
ROGERS JOSEPH O'DONNELL, PC
311 California Street, 10th Floor
San Francisco, CA 94104
(415) 956-2828
rgoodman@rjo.com
lsujeeth@rjo.com

Sehreen Ladak (Bar No. 307895)
PROSKAUER ROSE LLP
2029 Century Park East, Suite 2400
Los Angeles, CA 90067-3010
(310) 284-5652
sladak@proskauer.com

Attorneys for Defendant Bright Data Ltd.
**Admitted Pro Hac Vice*